(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 335 563 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
13.08.2003 Bulletin 2003/33

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/22

(21) Application number: **03250701.4**

(22) Date of filing: **04.02.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT SE SI SK TR
Designated Extension States:
AL LT LV MK RO

(30) Priority: **06.02.2002 US 66699**

(71) Applicant: **Xerox Corporation**
Rochester, New York 14644 (US)

(72) Inventors:
- **Balfanz, Dirk**
  Menlo Park, CA 94025 (US)
- **Lopes, Cristina V.**
  San Francisco, CA 94132 (US)
- **Smetters, Diana K.**
  Burlingame, CA 94010 (US)
- **Stewart, Paul Joseph**
  Sunnyvale, California 94087 (US)
- **Wong, Hao-Chi**
  San Carlos, CA 94070 (US)

(74) Representative: **Skone James, Robert Edmund**
GILL JENNINGS & EVERY
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) Method for securing communication over a network medium

(57) Pre-authentication information of devices (310,320) is used to securely authenticate arbitrary peer-to-peer ad-hoc interactions. In one embodiment, public key cryptography is used in the main wireless link (340) with location-limited channels (330) being initially used to pre-authenticate devices.

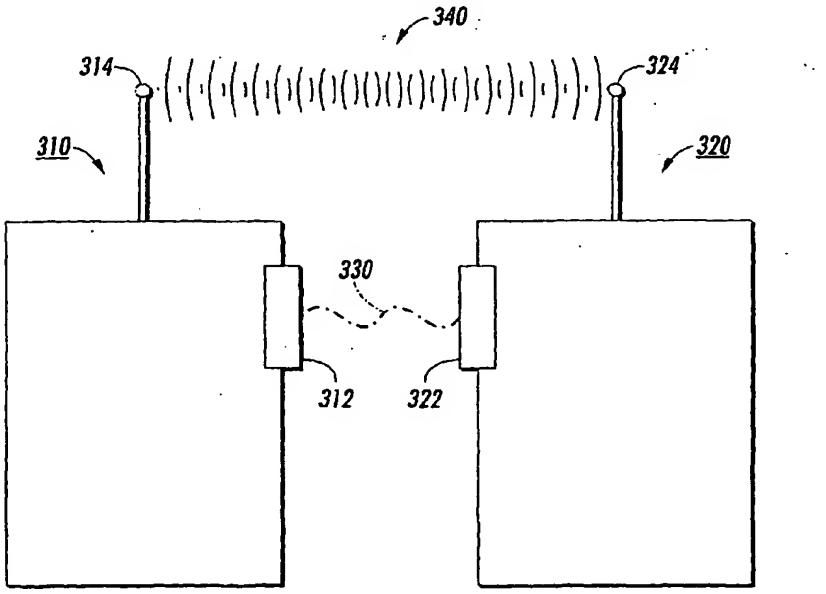

FIG. 1

EP 1 335 563 A2

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] Network communications have enabled users to receive information, such as documents, over the network medium. The network medium includes wired networks and wireless networks. Information transmitted over the network medium may be accessible to others. However, users typically desire that such information received not be available to others.

[0002] In one known example, the user wants to print a sensitive document that the user just received on the user's wireless device.

[0003] To do this, the user needs to let the wireless device know how to find the first printer over a wireless medium, such as a wireless network. Conventionally, there are few options user may use to find the first printer. Assuming each printer has a unique name, the user may type the name of the first printer into the user's wireless device. Alternatively, the user may have access to a discovery protocol, where the user may pick the first printer out of a list of printers. But the wireless device should guarantee that it is actually talking to the first printer and that the communication is secure.

[0004] If the first printer has a certificate issued by a trusted authority the wireless device may perform a key exchange with the first printer and establish an authenticated and secret channel with the first printer. However, several problems are associated with this approach. For instance, an immense public key infrastructure may be required and every printer, including potential participants of the public key infrastructure, may require a unique name with a certificate being issued by the trusted authority. This is typically very expensive. Further, an immense public key infrastructure may not be practical.

[0005] Another method may be to use an out-of- band mechanism for establishing security. Frank Stajano et al., "Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," 7th International Workshop, Lecture Notes in Computer Science, Cambridge, United Kingdom, April 1999, Springer-Verlag, Berlin, Germany, describes a security model usable to regulate secure transient association between devices in ad-hoc wireless networks.

[0006] In accordance with the present invention, a method for securing a communication over a network medium between at least two devices comprises transmitting pre-authentication information from a first device to a second device over a location-limited channel; and

using the pre-authentication information secured by the second device to authenticate the communication from the first device.

[0007] This invention provides systems and methods that allow a communication between a plurality of devices to be secured.

[0008] Location-limited communication channels are used to transmit the pre-authentication information between the plurality of devices.

[0009] In various exemplary embodiments, a software framework that supports inclusion of different location-limited channel types, public key algorithms used for the key exchange protocols and the final key exchange protocols chosen, and allows these to be dynamically chosen, can be used. The framework can be extended, to provide a new location-limited channel type, or a new key exchange protocol for example, by implementing a Java™ interface to provide a small amount of syntactic "glue".

[0010] The framework provides both client and server components, and allows developers to choose from either low-level, step-by-step control over data exchange, or to use simpler, higher-level interfaces. Such interfaces, for instance, provide server threads that can manage pre-authentication of multiple clients over the location-limited channel, and offer control over how such pre-authentication information is used to authenticate those clients over the wireless link. Framework components maintain state tracking regarding which devices have currently pre-authenticated, what keying information is currently in use by a particular device, and the like.

[0011] In various exemplary embodiments, a system comprises a client, which is the initiator of the authenticated channel, and a responding server. The server listens for a connection on both the location-limited channel and the primary link, but only admits primary-link connections from clients who have performed pre-authentication on the location-limited channel.

[0012] In various exemplary embodiments, the commercially-available Infra-red Data Association (IrDA) system can be used as a medium for the location-limited channel. The client opens an IrDA connection to the server, and generates an error if it discovers more than one potential IrDA endpoint. Across this connection, the client and the server exchange pre-authentication data such as, for example, XML-encoded pre-authentication data, containing pre-authentication information, such as, for example, a commitment to an ephemeral Digital Signature Algorithm (DSA) public key, a "friendly name", and an IP address and a port on which the server is listening.

[0013] With the pre-authentication complete, the IR channel is closed, and the client extracts the server's IP address and port number from the data it received. The client opens a normal SSL/TLS connection to the server on the primary link. Each side uses the information gained in the pre-authentication step, i.e., the commitments to the public keys, to authenticate the newly opened channel. The client and server are now free to securely exchange any information they choose over the primary link.

[0014] These and other features and advantages of the invention are described in, or are apparent from, the following detailed description of various exemplary embodiments of the systems and methods according to this invention.

Fig. 1 illustrates an example of a communication au-

thenticating system according to this invention;
Fig. 2 illustrates an example of a wireless device according to this invention;
Fig. 3 is a flowchart of a method for authenticating communication over a wireless medium;
Figs. 4-6 is another flowchart of a method for authenticating communication over a wireless medium;
Figs. 7-9 illustrate a communication authenticating system for a group of devices;
Fig. 10 is a flowchart of a method for authenticating communication over a wireless medium; and
Fig. 11 is another flowchart of a method for authenticating communication over a wireless medium.

[0015] According to this invention, pre-authenticating a number of wireless devices is used to securely authenticate arbitrary peer-to-peer ad-hoc interactions. This may include a bootstrap to a key exchange protocol that is used to set up an encrypted channel. A public key is committed to on the pre-authentication channel. A key exchange protocol using public key cryptography is used in the main wireless link to establish secure communications. Due to pre-authenticating the wireless devices using public keys, the types of media usable as location-limited channels do not need to be immune to eavesdropping and can include, for example, audio and/or infra-red channels. Pre-authenticating the wireless devices using public keys allows a range of public-key-base key exchange protocols which can authenticate wireless devices to be used.

[0016] Fig. 1 illustrates one exemplary embodiment of a wireless system 300. Only two wireless devices 310 and 320 are shown. However, the system 300 is capable of including more than two wireless devices. The first wireless device 310 includes a location-limited channel receiver/transmitter 312 and a main wireless link receiver/transmitter 314. Likewise, the second wireless device 320 includes a location-limited channel receiver/transmitter 322 and a main wireless link receiver/transmitter 324. In an alternative embodiment, the first and second wireless devices each has a main wired link receiver/transmitter, such as Transport Control Protocol/ Internet Protocol (TCP/IP) sockets or any other known or later developed wired network receivers/transmitter. In another embodiment, the first and second wireless devices have both a main wireless link and a main wired link.

[0017] If the first wireless device 310 initiate communication with the second wireless device 320, the first wireless device 310 initially sends pre-authentication information through the location-limited channel receiver/transmitter 312 to the second wireless device 320 via the location-limited channel 330. The second wireless device 320 receives the pre-authentication information from the first wireless device 310 through the location-limited channel receiver/transmitter 322.

[0018] Where mutual authentication is not required, the first wireless device 310 does not need to send pre-authentication information to the second wireless device 320. A wireless device that does not mutually exchange pre-authentication information with another wireless device cannot authenticate the communication received from the other wireless device. Thus, that wireless device is unprotected against attacks by an eavesdropper. Thus, where mutual authentication is required, such as an exchange of sensitive information between two wireless devices, the second wireless device 320 responds by sending additional pre-authentication information through the location-limited channel receiver/transmitter 322 to the wireless device 310 via the location-limited channel 330.

[0019] The first wireless device 310 receives the pre-authentication information through its location-limited channel receiver/transmitter 312. With the pre-authentication information exchanged between the first and second wireless device 310 and 320, the first wireless device 310 uses the main wireless link receiver/transmitter 314 to communicate with the second wireless device 320 via the main wireless link 340. The second wireless device 320 uses its main wireless link receiver/transmitter 324 to communicate with the first wireless device 310 via the main wireless link 340. Because pre-authentication information has been exchanged between the two wireless devices 310 and 320 in both directions, each of the first and second wireless devices 310 and 320 authenticates the communication of the other wireless device 320 and 310, respectively, using the received pre-authentication information received from that other wireless device 320 or 310, respectively.

[0020] Fig. 2 illustrates one exemplary embodiment of a wireless device 400. The wireless device 400 may be a Personal Digital Assistant (PDA), a laptop computer with wireless capability, a wireless hand held computer, a Blackberry™ device, a printer with wireless capability, a wireless phone and the like. The wireless device 400 includes a processor 410, a memory 420, an input/output (I/O) interface 430, a location-limited channel receiver/transmitter 442 and a main wireless link receiver/transmitter 444.

[0021] The memory 420 stores an operating system 422, a wireless application 424, an authentication application 426 and an authenticator 428. The operating system 422 provides the computer instructions which, when executed by the processor 410, programs and controls various I/O controllers including the I/O interface 430 of the wireless device 400. The operating system 422 provides instructions that stores the wireless application 424, the authentication application 426 and the authenticator 428 in a retrievable manner.

[0022] The wireless application 424 provides instructions that, allows the wireless device 400 to communicate with a wireless network through the main wireless link receiver/transmitter 444 connected to a main wireless link interface 434 of the I/O interface 430. The wireless application 424 may be Bluetooth™, ANSI/IEEE 802.11, and the like.

[0023] A wireless receiver/transmitter and interface used in a wireless network can be used as the main wireless link interface 434 and the main wireless link receiver/transmitter 444. In an alternative embodiment, the wireless device has main wired link interface and main wireless link receiver/transmitter such as TCP/IP interface and socket or both the main wireless link interface and transmitter, and main wired interface and receiver/transmitter.

[0024] The location-limited channel receiver/transmitter 442 may be separate from the main wireless link receiver/transmitter 444. A suitable location-limited channel receiver/transmitter 442 has at least two properties in order to send and receive pre-authentication information of the wireless devices. The first such property is a demonstrative property. A suitable location-limited channel receiver/transmitter 442 has physical limitations in its transmissions. For example, sound, whether in the audible and/or in the ultrasonic range, which has a limited transmission range and broadcast characteristics, may be used as a location-limited channel for a group of wireless devices. For point-to-point communication, such as between two wireless devices, a location-limited channel with directionality, such as an infrared channel may be used. The demonstrative property allows for communication across a location-limited channel to "name" a target device or group of devices based on the physical relationships between the devices and the limited locations accessible through the location -limited channel.

[0025] The second property is authenticity. This property ensures that pre-authentication information exchanged over the location-limited channel allows the exchanging wireless devices to securely authenticate each other over the main wireless link, even in the presence of eavesdroppers. If the participants use the location-limited channel to exchange their public keys as pre-authentication information, an attack by an eavesdropper on location-limited channel does not matter because the eavesdropper does not know the participants' private keys. The participants will authenticate each other over the main wireless link by proving possession of their corresponding private keys as part of a key exchange protocol. Thus, the eavesdropper will not be able to impersonate any of the participants.

[0026] Another property of a location-limited channel receiver/transmitter is that the location-limited channel is difficult to attack without the attack being detected by at least one legitimate participant (human or device). These include a receiver/transmitter that uses infra-red, sound, whether audio and/or ultrasound, and/or near-field signaling across the body.

[0027] Detecting the attack may not require that the devices transmitting on the location-limited channel be identified. Instead, for example, detecting the attack may merely depend on one's ability to count. Thus, if two wireless devices are attempting to communicate, and the communication is successful, as indicated, for example, by the lights on the target device blinking, or by the human that is using a laptop computer indicating that the communication was successful, then the number of legitimate participants are known. If extra, illegitimate, participants are detected, for example, by the laptop indicating that a third participant has joined the communication, the communication may simply be aborted by the legitimate participants.

[0028] The pre-authentication information is used to authenticate the received authenticator 428. The authenticator 428 may be a key, a secret, or the like. The key may be either a long-lived key or an ephemeral key. The choice is usually based on the application in which the key is being used. In either case, the key does not require certification by a trusted authority. However, if the key exchange protocol chosen requires an exchange of certificates, the certificate may be self-signed by the wireless device 400.

[0029] Usually, the amount of information exchanged across the location-limited channel is a small fraction of the amount of information sent across the main wireless link. One method of reducing the size of the pre-authentication information is to use cryptographically-secure hash functions, such as, for example, Secure Hash Algorithm-1 (SHA-1). Using this method, the participants need not actually exchange their complete public keys as pre-authentication information. Instead the participants send commitments of the keys, for example, by exchanging digests of the keys. The participants exchange commitments to their public keys across a chosen location-limited channel. In doing so, each participant is able to identify whom that participant is communicating with.

[0030] The wireless device 400 communicates with another wireless device using the main wireless link receiver/transmitter 444. The wireless device 400 uses the authentication application 426, which may include various established public-key-based key exchange protocol, such as the commercially available Secure Socket Layer/ Transport Layer Security (SSL/TLS), Secure Key Exchange Mechanism (SKEME), Internet Key Exchange (IKE) and the like, to prove possession of the private key, which corresponds to the public key committed during the pre-authentication information exchange. In the case, where a digest of the public key was sent during the pre-authentication information exchange, the wireless device 400 exchanges the complete public key over the main wireless link. The key exchange may either be prefixed to protocol execution, or, as in Socket Layer/ Transport Layer Security (SSL/TLS), occurs naturally as a standard part of the key exchange protocol. The keys are authenticated by the fact that they were the ones committed to across the location-limited channel. The wireless device 400, having authenticated the other wireless device's public keys, proceed with the exchange protocol on the main wireless link.

[0031] Fig. 3 is a flowchart outlining one method for

authenticating a communication over a network medium. The first wireless device contains a first public key PK_1. The second wireless device contains a second public key PK_2. Beginning in step S100, operation continues to step S110, where first wireless device sends a commitment to the public key PK_1 using a location-limited channel to a second wireless device. This is at least a part of the exchange of pre-authentication information over the location-limited channel. The commitment can be the public key itself, a certificate, or a digest of the public key. Then, in step S120, in response to receiving the commitment to the public key PK_1 from the first wireless device, the second wireless device sends a commitment to the public key PK_2 over the location-limited channel, which is received by the first wireless device. At this stage, the first wireless device may also receive the address of the second wireless device to provide for communication over the main wireless link.

[0032] In step S130, the first wireless device sends the public key PK_1 to the second wireless device using the wireless main link. In step S140, the second wireless device sends its public key PK_2 to the first wireless device and the exchange of keys take place. In step S150, the first wireless device authenticates the public key PK_2 received from the second wireless device and compares the public key PK_2 against the commitment received in the pre-authentication information stage. In one embodiment, the authentication of the received public key PK_2 is performed using a key exchange protocol, such as those illustrated in Fig. 2, that proves ownership of a private key corresponding to the public key. In the event that the second wireless device is using a secret S_2 when the first wireless device sends its public key PK_1 across the wireless main link the second wireless device verifies the public key PK_1 against the commitment, and uses it to encrypt its secret S_2 and returns the result $EPK_1(S_2)$ to the first wireless device. Authentication is performed by the second wireless device's ability to produce the secret S_2, and the first wireless device's ability to decrypt the result $EPK_1(S_2)$.

[0033] In step S160, a determination is made whether the commitment for the public key PK_2 previously received from the second wireless device matches the received public key PK_2. If so, operation continues to step S170. Otherwise, operation jumps to step S180. In step S170, the first wireless device resumes communication with the second wireless device over the main wireless link using the symmetric key agreed upon during the key exchange protocol to encrypt the communication. Operation then jumps to step S190. In contrast, in step S180, if the first wireless device cannot authenticate the public key PK_2 of the second wireless device the first wireless device terminates the communication with the second wireless device. Operation then continues to step S190, where the method ends.

[0034] It should be appreciated that in various exemplary embodiments, the first wireless device includes an arbitrary secret S_1, such as a random number. In this case, because the first wireless device is sending a commitment to the arbitrary secret S_1, the commitment is sent in a form of a cryptographic digest $h(S_1)$ because S_1 is to remain a secret. In various other exemplary embodiments, the first wireless device may also transmit its address, such as an IP address and port number, a Bluetooth device address, a user-friendly name or any other appropriate information to provide for communication at the main wireless link.

[0035] Figs. 4-6 are a flowchart outlining one exemplary embodiment of a method that complements an improved Guy Fawkes protocol that provides for interactive communication. This method may be used where the wireless devices have limited computational resources, such that public key operations are infeasible, and the location-limited channel does not provide a trusted exchange of secret data.

[0036] An example of a conventional Guy Fawkes protocol is described in Anderson et al., "A New Family of Authentication Protocols", ACMOSR: ACM Operating Systems Review, 32, 1998. Initially designed for authenticating digital streams the Guy Fawkes protocol assumes that parties A and B want to exchange streams, comprising sequential blocks $A_0,A_1,A_2,\ldots$ and $B_0,B_1,B_2,\ldots$ respectively. At each step i, A sends to B a packet P_i containing 4 pieces of data: a block A_i; a random value X_i, used as an authenticator for the block A_i; the digest $X_{i+1}h(X_i+1)$ of the next authenticator; and the $n(a_i+1)$ digest of the message $a_{i+1} = "(A_{i+1},h(X_{i+2}),X_{i+1})"$. B does the same during that step i. Assuming that B received an authenticated packet P. B authenticates the packet Pi as soon as B receives it, because the packet Pi contained the digest $n(a_{i+1})$. It should be appreciated that this does not hold if A and B do not execute in lock-step. Thus, this protocol requires both A and B to know, one step ahead of time, what they want to say next, which makes the protocol unsuitable for interactive exchanges.

[0037] As shown in Figs. 4-6, operation begins in step S200 and continues to step S205, where a counter N is set to 1. In step S210, a first wireless device sends an N^{th} communication that includes a digest of its N^{th} secret (authenticator) that will be used to authenticate its N^{th} message together with a digest of its N^{th} message over a location-limited channel to a second wireless device. In step S215, the second wireless device sends an N^{th} communication that includes a digest of its N^{th} secret that will be used to authenticate its N^{th} message together with a digest of its N^{th} message over the location-limited channel to the first wireless device.

[0038] In step S220 the first wireless device sends a digest of the N^{th} communication of the second wireless device and the first wireless device's N^{th} secret to the second wireless device. In step 225, the second wireless device sends a digest of the N^{th} communication of the first wireless device and the second device's N^{th} secret to the first wireless device. In step S230, a determination is made by one or both of the first and second

wireless devices whether to terminate the communication. If either of the first wireless device or the second wireless device determines to terminate the communication, operation proceeds to step S320. Otherwise, the communication continues and operation continues to step S235.

[0039] In step S235, the first wireless device continues the communication over a main wireless link. As the initiator of the communication, the first wireless device sends an N^{th} message which is meaningful, and a digest of its $(N+1)^{th}$ secret that will be used to authenticate its $(N+1)^{th}$ message together with an $(N+1)^{th}$ communication that includes a digest of the $(N+1)^{th}$ message to the second wireless device. In step S240, the second wireless device sends an N^{th} message which is meaningless, and a digest of its $(N+1)^{th}$ secret that will be used to authenticate its $(N+1)^{th}$ message together with an $(N+1)^{th}$ communication that includes a digest of the $(N+1)^{th}$ message to the first wireless device. The N^{th} message of the second wireless device is meaningless because the N^{th} message was committed to in step S215, when the second wireless device did not know the N^{th} message of the first wireless device that was transmitted in step S210. At this point, either of the wireless device can terminate the communication. Accordingly, in step S245, a determination is made by one or both of the first and second wireless devices whether to terminate the communication. In either of the first wireless device or the second wireless device determines to terminate the communication, operation proceeds to step S320. Otherwise, the communication continues and operation continues to step S250.

[0040] In step S250, the first wireless device sends a digest of the second wireless device's $(N+1)^{th}$ communication and the first wireless device's $(N+1)^{th}$ secret to the second wireless device. In step S255 the second wireless device sends a digest of the first wireless device's $(N+1)^{th}$ communication and the second device's $(N+1)^{th}$ secret to the first wireless device.

[0041] In step S260, the first wireless device sends an $(N+1)^{th}$ message which is meaningless, and a digest of its $(N+2)^{th}$ secret that will be used to authenticate its $(N+2)^{th}$ message together with a $(N+2)^{th}$ communication that includes a digest of the $(N+2)^{th}$ message to the second wireless device. The $(N+1)^{th}$ message of the first wireless device is meaningless because it is the second wireless device's turn to send a message which is meaningful. In step S265, the second wireless device sends an $(N+1)^{th}$ message which is meaningful, and a digest of its $(N+2)^{th}$ secret that will be used to authenticate its $(N+2)^{th}$ message together with a $(N+2)^{th}$ communication that includes a digest of the $(N+2)^{th}$ message to the first wireless device. The second wireless device sends the message that is meaningful due to the commitment made in step S240 after the second wireless device learned of the N^{th} message of the first wireless device that was meaningful. In step S270, a determination is made by one or both of the first and second wireless devices whether to terminate the communication. In either of the first wireless device or the second wireless device determines to terminate the communication, operation proceeds to step S320. Otherwise, the continues operation and continues to step S275.

[0042] In step S275, the first wireless device sends a digest of the second wireless device's $(N+2)^{th}$ communication and the first device's $(N+2)^{th}$ secret to the second wireless device. Next in step S280, the second wireless device sends a digest of the first wireless device's $(N+2)^{th}$ communication and the second device's $(N+2)^{th}$ secret to the first wireless device. In step S285, the first wireless device sends an $(N+2)^{th}$ message that is meaningless, and a digest of its $(N+3)^{th}$ secret that will be used to authenticate its $(N+3)^{th}$ message together with a $(N+3)^{th}$ communication that includes a digest of the $(N+3)^{th}$ message to the second wireless device. The $(N+2)^{th}$ message is meaningless because the first wireless device was committed in step S260 when the first wireless device had not received the $(N+1)^{th}$ message of the second wireless device that was meaningful. However, the first wireless device can commit to the $(N+3)^{th}$ message that is meaningful because the first wireless device had the $(N+1)^{th}$ message from the second wireless device in step S265 that was meaningful.

[0043] In step S290, the second wireless device sends an $(N+2)^{th}$ message that is meaningless, and a digest of its $(N+3)^{th}$ secret that will be used to authenticate its $(N+3)^{th}$ message together with a $(N+3)^{th}$ communication including a digest of the $(N+3)^{th}$ message to the first wireless device. The $(N+2)^{th}$ message of the second wireless device is meaningless because the next turn to "talk" belongs to the first wireless device. Again, at this point, either of the wireless devices can terminate the communication. Accordingly, in step S295, a determination is made by one or both of the first wireless device and the second wireless device whether to terminate the communication. If either of the first wireless device or the second wireless device determines to terminate the communication, operation jumps to step S320. Otherwise, the communication continues and operation continues to step S300.

[0044] In step S300, the first wireless device sends a digest of the second wireless device's $(N+3)^{th}$ communication and the first device's $(N+3)^{th}$ secret to the second wireless device. In step S305, the second wireless device sends a digest of the first wireless device's $(N+3)^{th}$ communication and the second device's $(N+3)^{th}$ secret to the first wireless device. In step S310, the controller N is incremented by 4. Operation then returns to step S235. In contrast, in step S320 operation of the method ends.

[0045] It should be appreciated that there are applications for which mutual authentication is not required. For instance, a device designed to provide a service to anyone that requests the service does not need to authenticate the device with which it is communicating, and therefore may be the only one to send pre-authen-

tication information. Such a device may have, for example, a passive beacon such as, for example, an Infrared (IR) beacon or Radio frequency Identification (RFId) tag, sending pre-authentication information that is sufficient to uniquely and securely identify its active proxy in wireless space. Such an approach may be used to add a measure of security and authentication to systems that use such beacons to provide a "digital presence" for physical objects.

[0046] Some of the location-limited channels described with respect to Fig. 4 have broadcast capability. Using such broadcast capabilities, protocols may be constructed that provide for authenticated group communication. Applications can include networked games and meeting support and/or conferencing software.

[0047] Audio is a medium that may provide a broadcast location-limited channel. Audio may be monitored and tracked by participants. Even if the participants in the exchange do not know what is carried in the audio messages, they can recognize the legitimate group participants that ought to be sending such audio messages. Audio may be incorporated into sounds that are already used by many pieces of software to provide feedback to participants. For example, most corporate conference call settings play a short "join tone" whenever a new participant enters a call. Such tones may be altered to also contain the participant's key information. Because designated channels designed to carry audio and/or voice information already exists, audio as a location-limited channel may be used via the telephone network.

[0048] Because using public key cryptography on location-limited channels means that those exchanges do not require secrecy, and thus are not vulnerable to eavesdropping, the broadcast characteristics of an audio channel may be used to pre-authenticate group communication. Each participant in the group communication broadcasts that participant's pre-authentication information over the audio channel, which is heard by all other legitimate participants. The preauthorization information will generally include a commitment to a public key. The broadcast may also be heard by attackers, but that poses no risk to the protocol's security unless those attackers also managed to broadcast their own pre-authentication information over the audio channel without detection by the legitimate participants, whether by humans or by devices. Any attackers so attempting to broadcast the attacker's information to mount an active attack on the location-limited channel will usually be detected by the legitimate human or device participants, because there will be an "extra" broadcast. For example, in the case of audio, there will be a broadcast from an unexpected location.

[0049] Legitimate participants proceed with known or later developed group key exchange protocol, where each participant proves, to one or more legitimate participants, that participant's possession of the private key corresponding to the public key committed to by the participant on the location-limited channel. Any participant capable of proving possession of the private key corresponding to one of the public keys so committed to is considered an authenticated participant in the group communication. Further, the chosen key exchange protocol may also result in all participants sharing a number of additional keys that can be used for encrypting and/or authenticating further communication between the participants of the group communication.

[0050] Figs. 7-9 illustrates an exemplary setting for authenticating a communication over a network medium among a group of wireless devices. As shown in Fig. 7, one participant acts as the group manager 610. The first participant to send pre-authenticate information becomes the group manager 610. Otherwise, a random participant is selected as the group manager. The group manager 610 broadcasts pre-authentication information, such as a commitment to a group public key, or its own public key, during a pre-authentication stage to various legitimate participants 612, 614 and 616 over a broadcast location-limited channel. As shown in Fig. 7, other parties 622, 624 and 626 are present and have access to the wireless network. Any attempt to send on the location-limited channel results in the detection of the attempt, because the legitimate participants are usually able to detect all transmissions on the location-limited channel, and are able compare the number of such transmissions with the number of expected transmissions, i.e., the number of legitimate participants.

[0051] As shown in Fig. 8, each participant 612, 614 and 616 responds to the pre-authentication broadcast information from the group manager 610 by each broadcasting that participant's own pre-authentication information, each containing a commitment to that participant's own public key, over the location-limited channel. These broadcasts are received by both the group manager 610 and the other legitimate participants 612, 614 and 616. After broadcasting that participant's pre-authentication information, each participant 612, 614, and 616 in turn makes a point-to-point connection to the group manager 610, for example, using the address provided by the group manager 610 as part of the group manager's pre-authentication information. Each participant 612, 614, and 616 engages with the group manager 610 in a point-to-point key exchange protocol, such as, for example Socket Layer/Transport Layer Security (SSL/TLS). Using the protocol, the group manager 610 gives each of the participants 612, 614, and 616 a copy of a shared group encryption key or keys. These keys are used to encrypt and authenticate further communication between all the participants, including the group manager 610 and the other participants 612, 614 and 616.

[0052] Because the parties 622, 624 and 626 did not broadcast their pre-authentication information on the location-limited channel, the group manager 610 does not recognize the parties 622, 624 and 626 as legitimate participants in the group communication. The parties 622, 624 and 626, therefore, will not be able to success-

fully create point-to-point connections on the main wireless link with the group manager, 610. This results in the parties 622, 624 and 626 not receiving the shared group key that would allow them to decrypt group communications between the legitimate participants including the group manager 610 and all the other participants 612, 614, and 616.

[0053] Fig. 10 is a flowchart outlining a first exemplary embodiment of a method for authenticating a communication over a network medium among a group of wireless devices.

Operation starts from step S400 to go to S410, where a group manager is selected for participants of the group. In step S420, the group manager broadcasts its pre-authentication information over a location-limited channel to the participants of the group. The pre-authentication information according to one embodiment may be a digest of a public key of the group manager. In step S430, each participant that receives the pre-authentication information of the group manager reciprocates by sending its pre-authentication information to the group manager and the other participants. The exchange of the pre-authentication information between the participants, including the group manager, occurs as a broadcast over the location-limited channel. According to one embodiment, the pre-authentication information of a participant is a digest of a public key of that participant.

[0054] In step S440, the group manager and each of the participants perform a point-to-point key exchange using the public keys corresponding to the digest of the public keys received during the pre-authentication stage, using any known or later-developed key exchange protocol over the wireless link, for example. Such a protocol will also set up a point-to-point encrypted and authenticated channel between the group manager and the current participants of the group. In step S450, the group manager may distribute to each participant over the wireless link a copy of a group key to be used as a shared session key. In step 460, operation of the authentication method ends, allowing for secure communication among participants of the group, including the group manager, to proceed.

[0055] In a centrally-managed group, managing the joining and leaving of participants may be relatively easy. A joining participant may use one of the two-party protocols discussed above with the group manager 610 to authenticate itself, and to receive the group key over a secured wireless link. When a participant leaves a group, the group manager 610 can distribute a new group key to all remaining participants over the wireless link. This may be done because the group manager 610 has established shared secret keys with each individual participant of the group during the point-to-point key exchange.

[0056] Fig. 11 is a flowchart outlining another method for authenticating a communication over a network medium among a group of wireless devices. The method outlined in Fig. 11 allows all participants to equally participate in key generation, and thus all participants may be equally trusted.

[0057] Operation begins in step S500 and continues to step S510, where each participant broadcasts its pre-authentication information, such as a commitment to a Diffie-Hellman public value, to the participants of the group using a broadcast location-limited channel. In step S520, each participant proceed with a chosen group key exchange protocol, where participants present their complete Diffie-Hellman public values over a wireless network. The group key exchange protocol may be a modified Diffie-Hellman key exchange among participants of the group, which allows all participants to share in the generation of the group shared secret key.

[0058] Like the standard two-party Diffie-Hellman key exchange, while a secret may be established, the participants of the group are strangers. Thus, these protocols based on extending Diffie-Hellman assume that all participants participate in a shared public key infrastructure, or have previously exchanged public keys.

[0059] Because pre-authentication information exchanged over the location-limited channels allows the participants to authenticate each other, this assumption is no longer necessary. The use of a broadcast location-limited channel allows all participants of the group to commit to their public keys publicly to one or more participants of the group. In step S530, the participants may then proceed with the chosen group key exchange protocol over the wireless link and, for example, use the presented complete Diffie-Hellman public values to derive a group key. Operation then continues to step S540, where operation of the authentication method ends, allowing secure communication to proceed.

[0060] A participant who joins in after a session has started may broadcast that participant's key commitment over the location-limited channel to the rest of the participants of the group as that participant joins. A randomly selected current participant can respond, providing mutual authentication. The chosen group key exchange protocol is used to handle the details of updating the shared group key for these new participants, or revoking keys of departing participants.

Claims

1. A method for securing a communication over a network medium between at least two devices, comprising:

   transmitting pre-authentication information from a first device to a second device over a location-limited channel; and

   using the pre-authentication information secured by the second device to authenticate the communication from the first device.

2. The method of claim 1, wherein transmitting the pre-

authentication information over a location-limited channel includes:

sending a commitment including at least a commitment to a first secret and a commitment to a meaningful message from the first device to the second device;
responding to the commitment from the first device by sending a commitment including at least a commitment to a second secret and a commitment to a meaningless message from the second device to the first device;
acknowledging receipt of the commitment of the second device by the first device; and
acknowledging receipt of the commitment of the first device by the second device.

3. A method according to claim 1 or claim 2, wherein the first and second devices form all or part of a group of devices, the method comprising:

designating at least one device of the group as a group manager;
exchanging pre-authentication information between the group manager and other devices of the group using a broadcast location-limited channel; and
using the exchanged pre-authentication information secured by the group manager and the other devices to authenticate the communication over the network medium.

4. The method of claim 3, further comprising using the network medium to distribute a group key information from the group manager to the other devices in the group.

5. The method of claim 3 or claim 4, further comprising:

receiving a new device into the group of devices;
exchanging pre-authentication information between the group manager and the new device using the broadcast location-limited channel; and.
using the exchanged pre-authentication information secured by the group manager and the new device to authenticate the communication over the network medium between the group manager, the group of devices and the new device.

6. The method of any of claims 3 to 5, wherein, when a device leaves the group of devices, the method further comprises:

nullifying pre-authentication information of the group manager with respect to remaining ones of the other devices of the group;
distributing new pre-authentication information by the group manager to the remaining devices in the group;
using the distributed pre-authentication information by the group manager and the remaining ones of the devices of the group to authenticate the communication between the group manager and the remaining ones of the devices of the group.

7. The method any of claims 3 to 6, further comprising using the network medium to distribute a new group key information from the group manager to the remaining ones of the devices of the group.

8. A method according to claim 1 or claim 2, wherein the first and second devices form all or part of a group of devices, the method comprising:

exchanging pre-authentication information between each device and other devices in the group over a broadcast location-limited channel; and
using the pre-authentication information of a selected device for communication that is secured by a communicating device to authenticate the communication over the network medium with the selected device.

9. A method according to any of the preceding claims, wherein an infra-red or audio channel is used as the location-limited channel.

10. A method accroding to any of the preceding claims wherein transmitting pre-authentication information includes sending a digest of an authenticator from one device to another device, the digest of the authenticator including one of a public key, a digest of the public key and a digest of a secret.

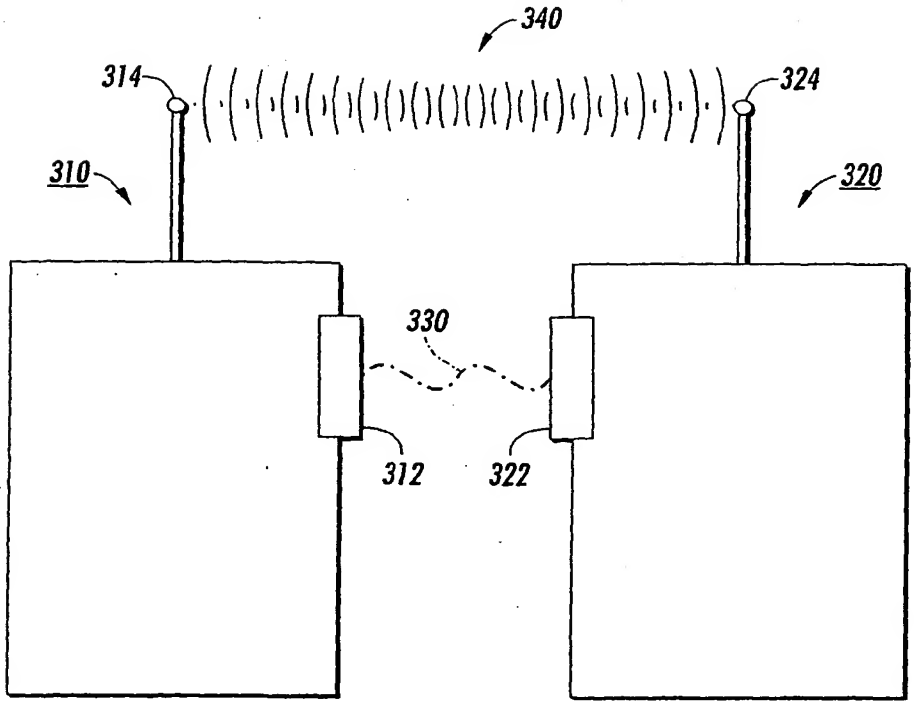

FIG. 1

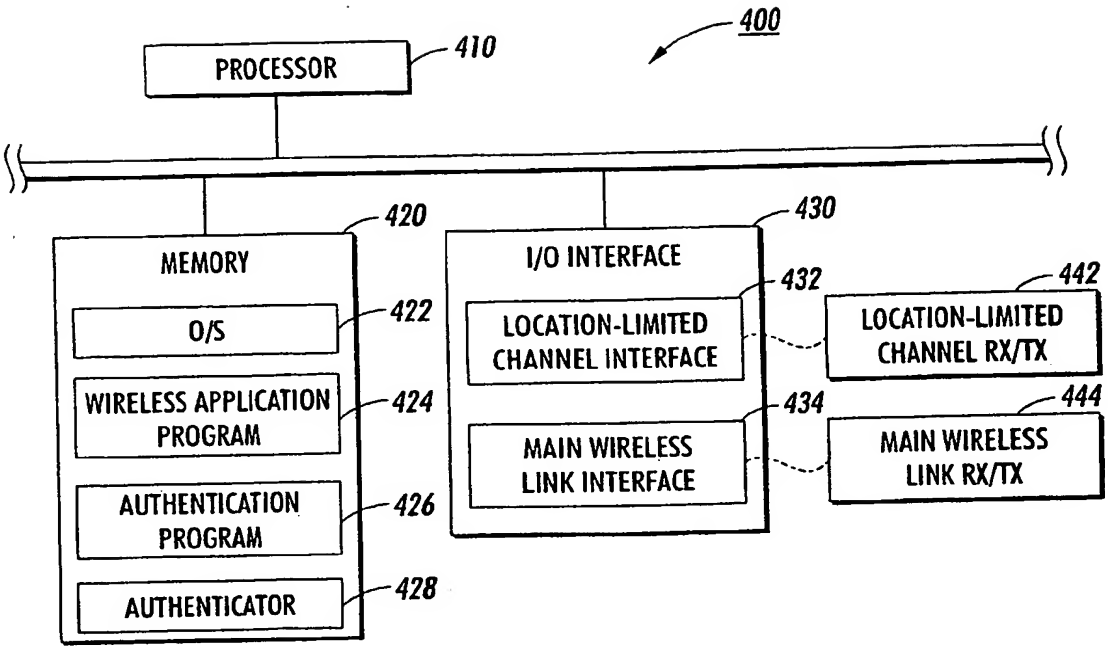

FIG. 2

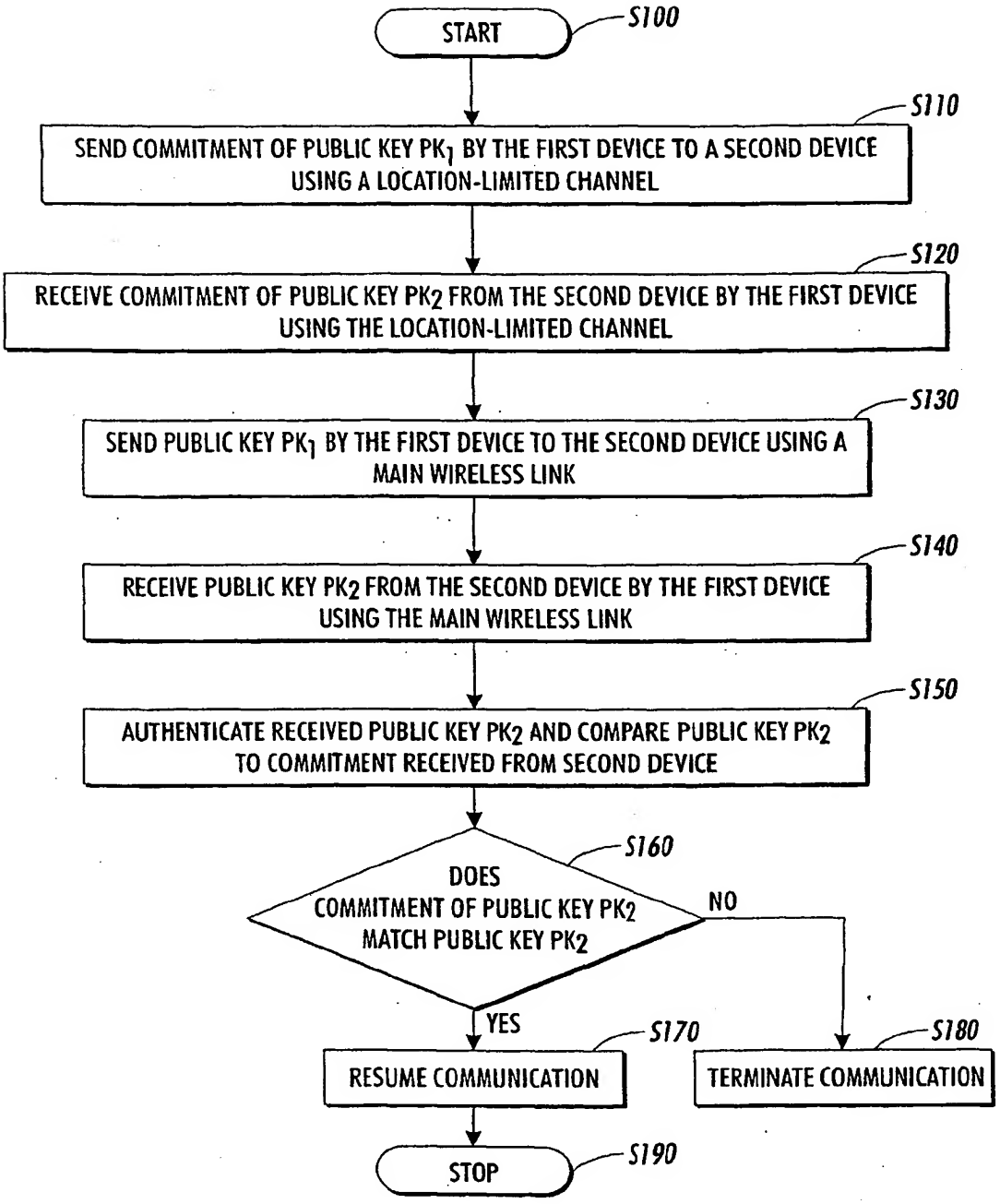

FIG. 3

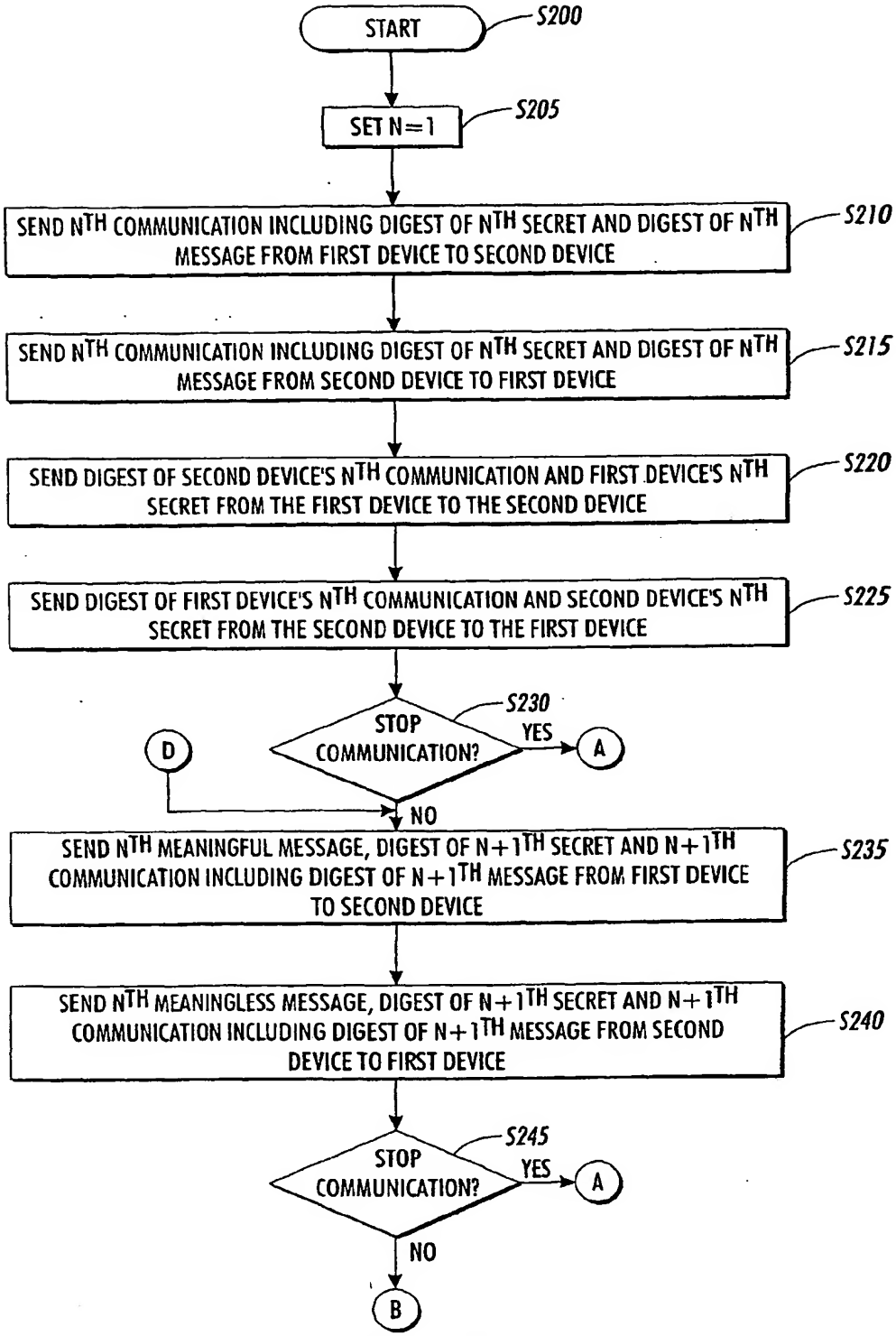

FIG. 4

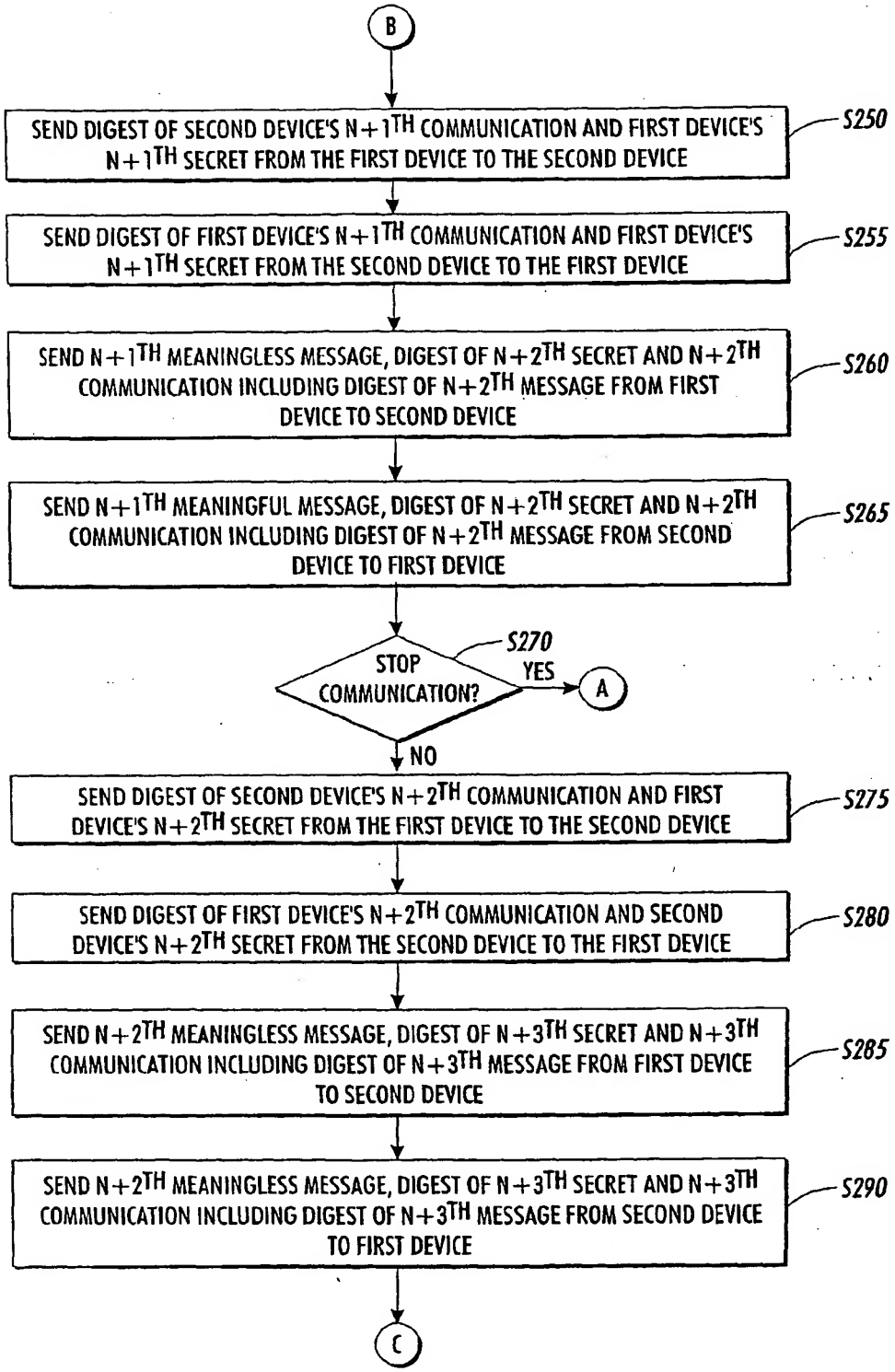

FIG. 5

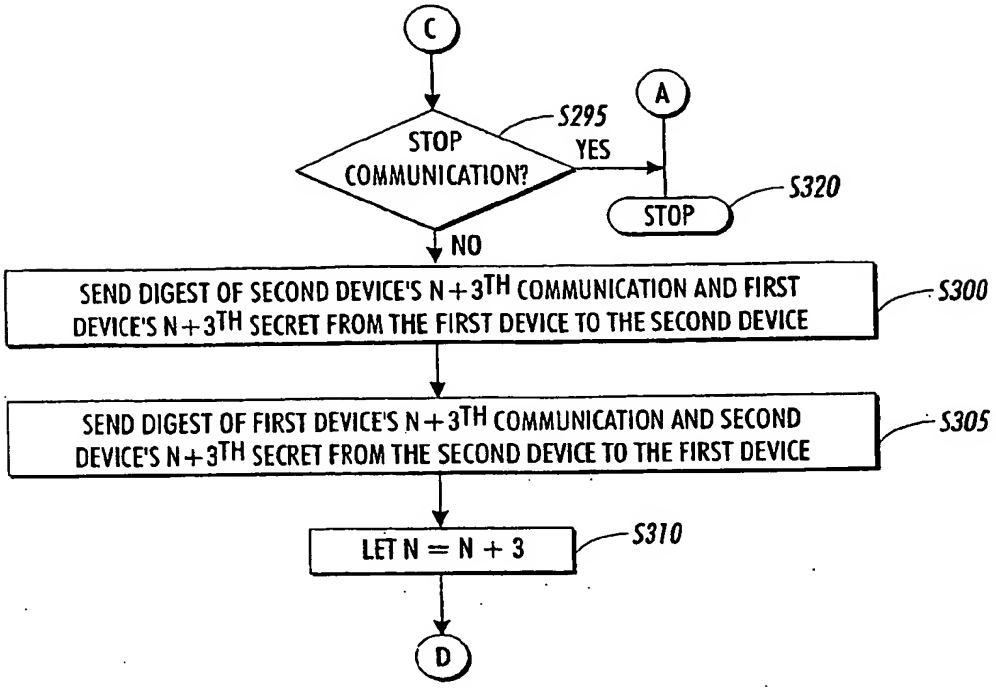

FIG. 6

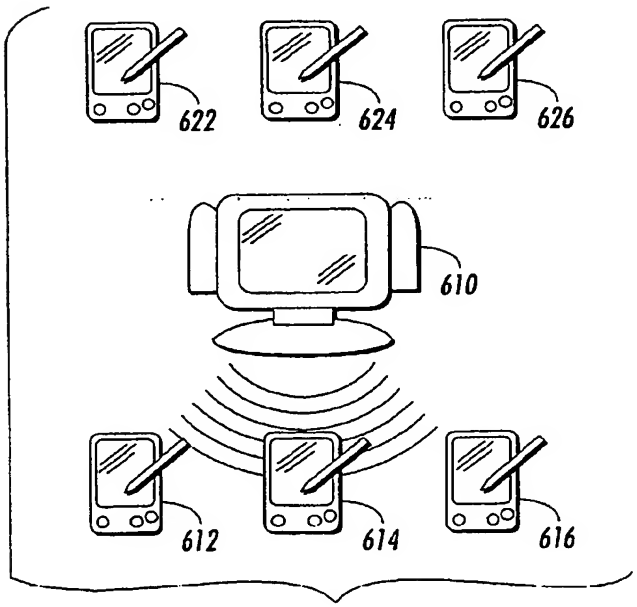

FIG. 7

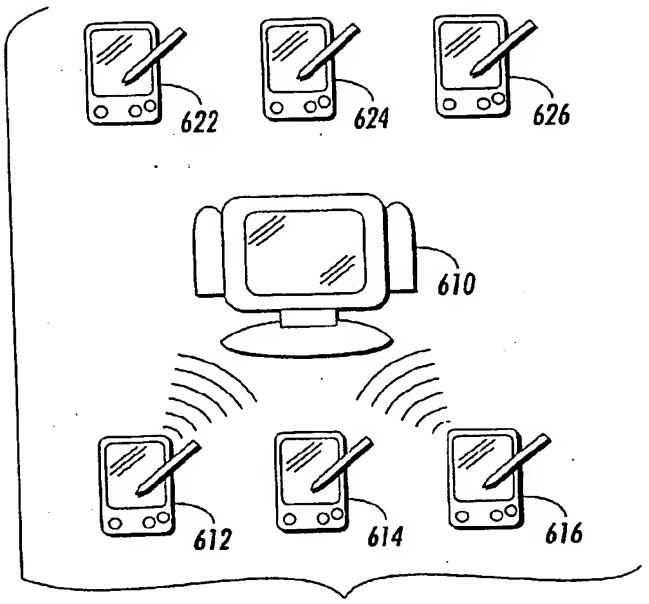

FIG. 8

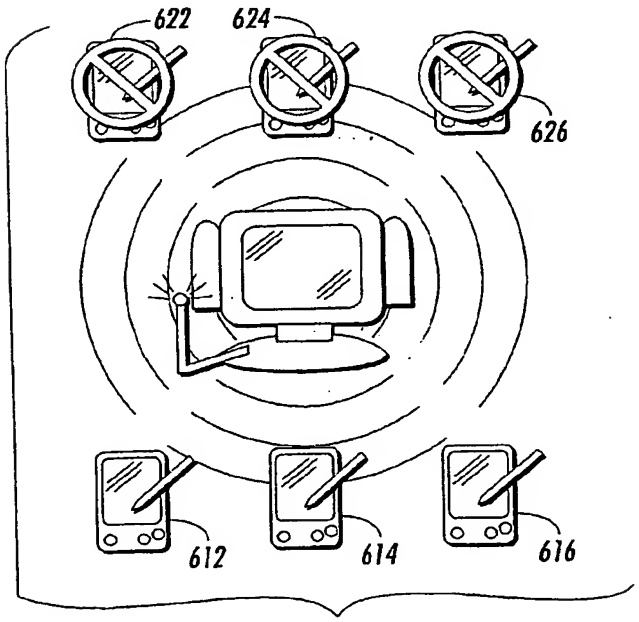

FIG. 9

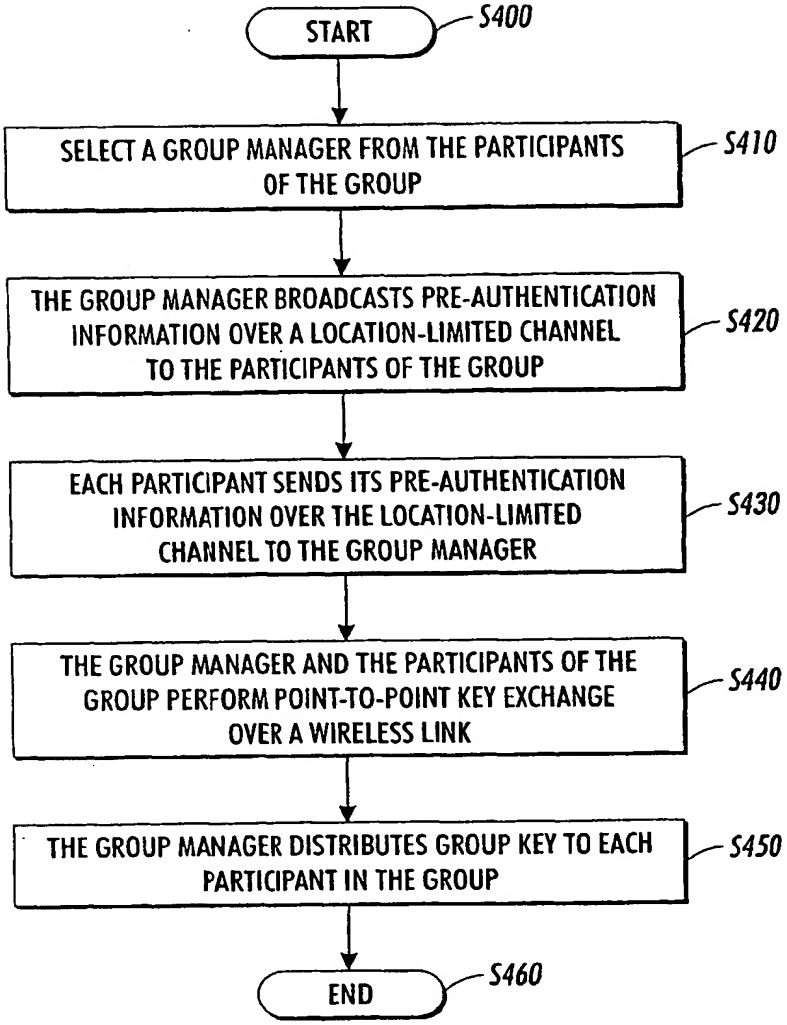

FIG. 10

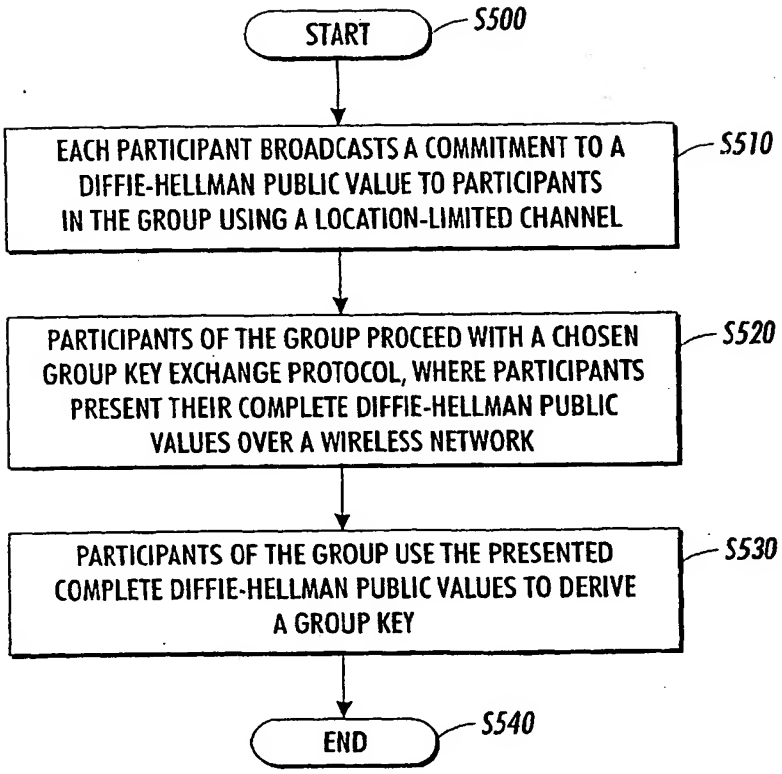

FIG. 11

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 335 563 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
15.10.2003 Bulletin 2003/42

(43) Date of publication A2:
13.08.2003 Bulletin 2003/33

(21) Application number: **03250701.4**

(22) Date of filing: **04.02.2003**

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/22

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT SE SI SK TR
Designated Extension States:
AL LT LV MK RO

(30) Priority: **06.02.2002 US 66699**

(71) Applicant: **Xerox Corporation**
Rochester, New York 14644 (US)

(72) Inventors:
- **Balfanz, Dirk**
  Menlo Park, CA 94025 (US)
- **Lopes, Cristina V.**
  Irvine, CA 92612 (US)
- **Smetters, Diana K.**
  Burlingame, CA 94010 (US)
- **Stewart, Paul Joseph**
  Sunnyvale, California 94087 (US)
- **Wong, Hao-Chi**
  San Carlos, CA 94070 (US)

(74) Representative: **Skone James, Robert Edmund**
GILL JENNINGS & EVERY
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) Method for securing communication over a network medium

(57) Pre-authentication information of devices (310,320) is used to securely authenticate arbitrary peer-to-peer ad-hoc interactions. In one embodiment, public key cryptography is used in the main wireless link (340) with location-limited channels (330) being initially used to pre-authenticate devices.

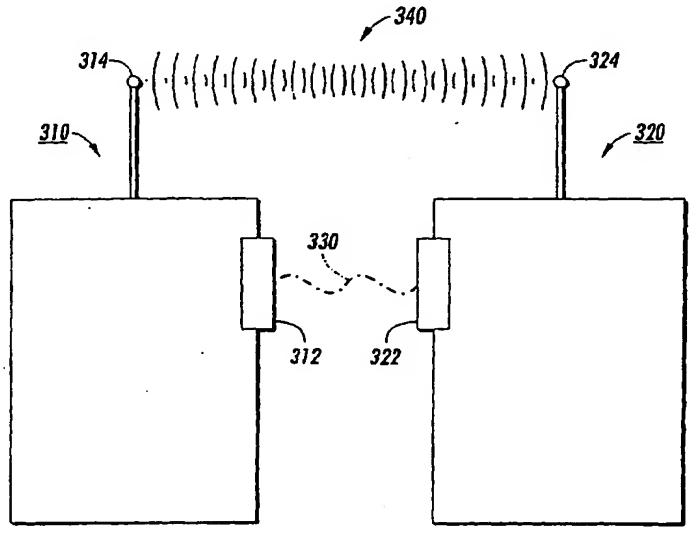

FIG. 1

EP 1 335 563 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 25 0701

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X Y	WO 99 41876 A (ERICSSON TELEFON AB L M) 19 August 1999 (1999-08-19) * abstract * * page 5, line 2-8 * * page 6, line 9-25 * * page 7, line 27 - page 10, line 5 * * page 11, line 24 - page 12, line 2 * ---	1,8-10 3-5,7	H04L29/06 H04L12/22
Y	ASOKAN N ET AL: "Key agreement in ad hoc networks" COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL, vol. 23, no. 17, 1 November 2000 (2000-11-01), pages 1627-1637, XP004238466 ISSN: 0140-3664 *Section 3.2 "Multi-party version"* *Section 4 "Deciding on leaders and ordering"* ---	3-5,7	
P,X	US 2002/065065 A1 (MOORE DAVID ET AL) 30 May 2002 (2002-05-30) * abstract * * paragraphs [0009]-[0011] * * paragraph [0046] * * paragraphs [0056]-[0059] * ---	1,8-10	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L H04B H04Q
A	F.STAJANO AND R. ANDERSON: "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks" 1999 AT&T SOFTWARE SYMPOSIUM, [Online] 15 September 1999 (1999-09-15), XP002245727 Retrieved from the Internet: <URL:www.uk.research.att.com/pub/docs/att/tr.1999.2b.pdf> [retrieved on 2003-06-24] * the whole document * --- -/--	1-10	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	12 August 2003	Olaechea, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 25 0701

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	BRUCE SCHNEIER: "Applied Cryptography:Protocols, Algorithms, and Source Code in C" 1996 , JOHN WILEY & SONS , NEW YORK, US XP002251019 275760 *Section 8.3 "Transferring Keys"* -----	10	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	12 August 2003	Olaechea, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 25 0701

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-08-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9941876 A	19-08-1999	US 6396612 B1	28-05-2002
		US 2002065099 A1	30-05-2002
		AU 748426 B2	06-06-2002
		AU 2650199 A	30-08-1999
		BR 9907826 A	24-10-2000
		CN 1290438 T	04-04-2001
		EE 200000467 A	15-02-2002
		EP 1055307 A1	29-11-2000
		JP 2002503920 T	05-02-2002
		WO 9941876 A1	19-08-1999
US 2002065065 A1	30-05-2002	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82